IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff and Counterclaim-Defendant, v. INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation, and SYMANTEC CORPORATION, a Delaware corporation, Defendants and Counterclaim- Plaintiffs.	Civil Action No. 04-CV-1199 (SLR) **FILED UNDER SEAL** THIS DOCUMENT CONTAINS MATERIALS WHICH ARE CLAIMED TO BE CONFIDENTIAL AND COVERED BY A PROTECTIVE ORDER. THIS DOCUMENT SHALL NOT BE MADE AVAILABLE TO ANY PERSON OTHER THAN THE COURT AND OUTSIDE COUNSEL OF RECORD FOR THE PARTIES

JOINT CLAIM CONSTRUCTION RESPONSE BRIEF OF DEFENDANTS ISS AND SYMANTEC

Richard L. Horwitz (#2246)
David E. Moore (#3983)
POTTER ANDERSON & CORROON LLP
Hercules Plaza, 6th Floor
1313 N. Market Street
Wilmington, DE 19899
Tel.: (302) 984-6000
Fax: (302) 658-1192

OF COUNSEL:
Holmes J. Hawkins III
Natasha H. Moffitt
KING & SPALDING LLP
191 Peachtree St.
Atlanta, GA 30303
Tel: (404) 572-4600
Fax: (404) 572-5145

Theresa A. Moehlman
KING & SPALDING LLP
1185 Avenue of the Americas
New York, New York 10036
Tel.: (212) 556-2100
Fax: (212) 556-2222

Attorneys for Defendant
INTERNET SECURITY SYSTEMS, INC., a Delaware Corporation and INTERNET SECURITY SYSTEMS, INC., A Georgia Corporation

Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
MORRIS, JAMES, HITCHENS & WILLIAMS, LLP
222 Delaware Avenue, 10th Floor
Wilmington, DE 19899-2306
Tel: (302) 888-6800
Fax: (302) 571-1751

OF COUNSEL:
Lloyd R. Day, Jr. (*pro hac vice*)
Robert M. Galvin (*pro hac vice*)
Paul S. Grewal (*pro hac vice*)
DAY CASEBEER MADRID & BATCHELDER LLP
20300 Stevens Creek Blvd., Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

Michael J. Schallop (*pro hac vice*)
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: (408) 517-8000
Fax: (408) 517-8121
Attorneys for Defendant
SYMANTEC CORPORATION

Original Date: June 30, 2006
REDACTED DATE: July 11, 2006

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Cases

TABLE OF AUTHORITIES (CONT.)

Page

Statutes

Pursuant to the Court's June 30, 2005 Scheduling Order, Defendants Internet Security Systems, Inc., a Delaware corporation, Internet Security Systems, Inc., a Georgia corporation (collectively "ISS") and Symantec Corporation ("Symantec") submit this joint response brief to Plaintiff SRI International, Inc.'s ("SRI's") opening brief on claim construction.

As discussed in Defendants' opening brief, in an effort to narrow the claim construction issues, Defendants have agreed on a single set of claim constructions. A chart showing the parties' consolidated claim construction proposals is attached.[1]

I. INTRODUCTION

SRI's proposed constructions fail to honor the principle that claims must be read *in light of the specification* and that a patentee cannot, for litigation purposes, enlarge what is patented beyond what it has described as the invention.

SRI's constructions ignore the specification's disclosure that the basic building block of the claimed hierarchical architecture is a generic *monitor* that is configured with a reusable module. By not using this basic definition, SRI's constructions do not adequately account for the specification's disclosure of the advantages of the alleged inventions: (1) the ability to form an analysis hierarchy of any depth or breadth; (2) the reduction of implementation and maintenance efforts by reusing generic software components; and (3) the ability to adapt the analysis by reconfiguring the monitors. Similarly, SRI's constructions ignore the specification's disclosure of a particular statistical detection method, and its purported advantages over other detection methods, such as signature matching.

---

[1] *See* Declaration of Geoffrey M. Godfrey in Support of Defendants' Joint Claim Construction Response Brief ("Godfrey Decl."), Ex. A.

In some instances, by failing to adopt the definitions of the specification, SRI's constructions render claims indefinite. For example, SRI's proposal that *monitor* be construed inconsistently within and among the claims makes it impossible to determine which version of SRI's *monitor* is to be applied to each claim element. In other instances, such as for the claim term *statistical detection method*, SRI's proposed constructions are circular and do little to clarify or explain what the patentee covered by the claims.

Defendants' proposed constructions should be adopted because they provide a more specific and meaningful explanation of the disputed claim terms, and account for the inventors' consistent use of those terms throughout the entire intrinsic record.

II. RESPONSE

A. Hierarchical Architecture Claims

As set forth in Defendants' opening brief, the patent defines the generic *monitor* as the building block of the disclosed architecture. SRI avoids this integral teaching in order to support its infringement theory. SRI proposes that *monitor/network monitor* be construed differently within and throughout the claims. SRI's constructions result in indefinite claims that lack clarity, are internally inconsistent and do not achieve the advantages of the alleged invention. In contrast, using Defendants' constructions, which properly reflect the entire intrinsic record, including the specification's definitions, the claims cohere internally and achieve the advantages of the alleged invention disclosed in the specification. The contrast is striking when the parties' constructions are viewed in the context of a full claim, as set forth in the attached chart.[2]

[2] *See* Godfrey Decl., Ex. B.

1. "network monitor"/"monitor"

Term	Defendants' Construction	SRI's Construction
network monitor / monitor	generic code that can be dynamically configured and reconfigured with reusable modules that define the monitor's inputs, analysis engines and their configurations, response policies and output distribution for its reports.	process or component in a network that can analyze data; depending on the context in specific claims, the network monitor may analyze network traffic data, reports of suspicious network activity or both. Service monitors, domain monitors and enterprise monitors are examples of network monitors.

Defendants' construction reflects how the terms *monitor/network monitor* are defined in the patents. Not only does the specification state that all *monitors* use the same generic code that is configurable with a reusable module, it uses that term consistently throughout the entire specification. "[W]hen a patentee uses a claim term throughout the entire patent specification, in a manner consistent with only a single meaning, he has defined that term 'by implication.'" *Bell Atl. Network Servs., Inc. v. Covad Communications Group, Inc.*, 262 F.3d 1258, 1271 (Fed. Cir. 2001) (citing *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)).

In order to avoid this result, SRI tries to characterize the monitor definition as merely the *preferred embodiment.* But that is not what the patent discloses — the generic monitor is a definition; the *preferred embodiment* is the configuration of those defined generic *monitors* into a three-tiered analysis hierarchy consisting of service monitors, domain monitors and enterprise monitors.[3] As SRI admits, these particular types of monitors are the disclosed *examples*:

[3] '338 patent at 3:32-4:20 [D.I. 268, Ex. C].

- "The claims of the '203, 212 and '615 patents require a hierarchical monitor (***examples*** of which are referred to in the specification as 'domain' and 'enterprise' monitors)."[4]

- "***[E]xamples*** of network monitors (16a-16f) include service monitors ..., domain monitors ..., and enterprise monitors."[5]

SRI's claim construction ignores the *monitor* definition in the specification. Unlike the generic monitor of Defendants' construction that is consistent with the specification, SRI's construction of *monitor/network monitor* could encompass potentially any entity in a network, regardless of whether that "component or process" (1) can be configured into any form of an analysis hierarchy, (2) makes use of reusable software, or (3) allows for reconfiguration. SRI "is not entitled to a claim construction divorced from the context of the written description." *Nystrom v. Trex Co.*, 424 F.3d 1136, 1144-45 (Fed. Cir. 2005).

Moreover, under SRI's construction, *monitor/network monitor* would be construed differently within and among the claims. SRI acknowledges the general rule that "the same term should be construed consistently in all claims in which it is used."[6] This is a basic, and well-established, rule of claim construction. *Callicrate v. Wadsworth Mfg., Inc.*, 427 F.3d 1361, 1371 (Fed. Cir. 2005). SRI contends that this is a rare case where the patent "so provides for" giving a claim term different meaning within and throughout the claims. But there is no support in the patents-in-suit for this argument.

---

[4] SRI's Opening Claim Construction Brief ("SRI's Br.") at 4 (emphasis added) [D.I. 265].

[5] *Id.* at 8 [D.I. 265].

[6] *Id.* at 8 n.7 [D.I. 265].

SRI's two cited cases on this point support Defendants' construction, not SRI's. In *CAE Screenplates Inc. v. Heinrich Fiedler GmbH & Co. KG*, 224 F.3d 1308, 1317 (Fed. Cir. 2000), the Court held that the claim term "plane" should be construed consistently. The patentee contended that the "upstream side plane" and the "downstream plane" referred to a physical structure, but "bottom plane" did not refer to a physical structure. The Court found the specification used "plane" consistently to refer to a physical structure and the patent did not teach otherwise. Similarly, here, the patent specification uses *monitor* consistently to refer to generic code that can be configured with a reusable module. Therefore, *monitor* should be construed consistently to require generic code that can be configured with a reusable module.

In the second case, *Epcon Gas Systems, Inc. v. Bauer Compressors, Inc.*, 279 F.3d 1022 (Fed. Cir. 2002), the two phrases were "substantially below" and "substantially constant." *Id.* at 1031. The Court found that "substantially below" denoted magnitude and "substantially constant" denoted approximation. *Id.* 1030-31. But the only reason the adjective "substantially" was held to have different meanings was because the patentee had narrowed the term in one context during prosecution. Specifically, the patentee had added the phrase "substantially below" to overcome prior art. *Id.* at 1031. Here, unlike in *Epcon Gas*, the term *monitor* is a structure, not a modifier, and SRI did not narrow its meaning in one context during prosecution.

Under SRI's construction, the meaning of *monitor* may differ "depending on the context in specific claims." SRI argues in its opening brief that "the function of the claimed monitors, including what specific type of data they must analyze, is defined contextually by the particular claim element in which 'network monitor' or 'monitor' is

used."[7] However, as shown in the accompanying chart showing the parties' constructions in the context of a full claim,[8] not all claim limitations using *monitor* provide sufficient context to enable one of skill in the art to figure out which *monitor* of SRI's construction applies and what component would meet the claim elements.

For example, under SRI's construction, it is unclear what components would meet the claims calling for a *hierarchical monitor* because it is unclear how hierarchical monitors get *deployed,* whether they must *generate reports* and whether, in addition to generating reports, they must also generate something called a *functional unit*, whatever that is. This ambiguity in SRI's *monitor* construction would render the claims indefinite under 35 U.S.C. § 112, ¶ 2. *See IPXL Holdings, L.L.C. v. Amazon.com, Inc.*, 430 F.3d 1377, 1383-84 (Fed. Cir. 2005) ("Section 112, paragraph 2, requires that the claims of a patent particularly point out and distinctly claim the subject matter which the applicant regards as his invention. A claim is considered indefinite if it does not reasonably apprise those skilled in the art of its scope.") (internal quotations omitted).

Moreover, under SRI's constructions, the dependent claims cannot be performed. For example, a domain monitor is a hierarchical monitor that feeds the enterprise monitor in the analysis hierarchy, and the dependent claims add *domain monitors* by further specifying the *deploying* step. However, under SRI's construction, hierarchical monitors such as domain monitors do not get deployed in that step. The claims thus do not cohere under SRI's constructions.

---

[7] SRI's Br. at 9 [D.I. 265].

[8] Godfrey Decl., Ex. B.

SRI argues that its construction would be the "plain and ordinary meaning . . . to one of ordinary skill in the art."[9] However, SRI offers no evidence that *monitor* had any "plain and ordinary" meaning to one skilled in the art as of November 1998, outside of the context of the patents-in-suit. The extrinsic evidence establishes that there was no such meaning and that one would therefore have had to rely on the definition provided in the specification to understand this term.

REDACTED

SRI's claim construction of *monitor/network monitor* should be rejected because it fails to achieve the advantages of the alleged invention and results in inconsistency and indefiniteness. Defendants' proposed construction should be adopted because it uses the definition provided in the specification, achieves the stated advantages, and results in consistency within and among claims.

---

[9] SRI's Br. at 7 [D.I. 265].

[10] Expert Report of Stephen E. Smaha at 19-20 [D.I. 266, Ex. G].

[11] *See* Lunt Tr. 232:11-20 [Godfrey Decl., Ex. C].

[12] Kesidis Tr. 504:10-22 [Godfrey Decl., Ex. D].

2. "deploying a plurality of network monitors"

Term	Defendants' Construction	SRI's Construction
deploying a plurality of network monitors	installing and configuring two or more network monitors so that together they form an analysis hierarchy defined by the network monitors' inputs and output distribution.	SRI does not believe the term needs construction but, if construed, should be construed to mean locating two or more network monitors so as to allow them to receive data to be monitored and/or to send information.

As Defendants discussed in their opening brief, the patents disclose that deploying network monitors includes installing and configuring them into an analysis hierarchy. SRI incorrectly asserts that Defendants' proposed constructions do not explain what configuration means.[13] As set forth in Defendants' construction of *monitor*, configuration includes defining each monitor's inputs, analysis engines and configuration, response policies, and output distribution. By setting the inputs and outputs of the monitors, a reporting structure (i.e., analysis hierarchy) is formed among the monitors. Defendants' constructions are in accord with the patent's disclosures concerning deployment:

- "[T]he enterprise 10 includes ***dynamically deployed*** network monitors 16a-16f that analyze and respond to network activity and can interoperate to form an analysis hierarchy."[14]
- "All monitors . . . use the same monitor code-base. . . . Customizing and ***dynamically configuring*** a monitor 16 thus becomes a question of building and/or modifying the resource object 32."[15]
- "The contents of the resource object 32 are defined and utilized during monitor 16 ***initialization***."[16]

---

[13] SRI's Br. at 21 n.10 [D.I. 265].

[14] '338 patent at 3:32-35 (emphasis added) [D.I. 268, Ex. C].

[15] *Id.* at 11:4-11 (emphasis added).

[16] *Id.* at 12:37-38 (emphasis added).

- "[T]he resource object 32 contains the operating parameters for each of the monitor's 16 components as well as the analysis semantics (e.g., the profiler engine's 22 measure and category definition, or the signature engine's 24 penetration rule-base) necessary to process an event stream. After defining a resource object 32 to implement a particular set of analyses on an event stream, the resource object 32 may be reused by other ***monitors 16 deployed*** to analyze equivalent event streams."[17]
- "The resource object 32 provides a pluggable configuration module for tuning the generic monitor code-base to a specific event stream. The resource object 32 includes configurable event structures 34 [that define the input of events to the monitor], analysis unit configuration 38a-38n, engine configuration 40a-40n, resolver configuration 42, decision unit configuration 44, subscription list data 46 [that indicates to which other monitors to send reports], and response methods 48."[18]
- "Upon its ***initialization***, the [monitor's] resolver 20 initiates authentication and subscription sessions with those monitors 16a-16f whose identities appear in the monitor's 16 subscription-list."[19]

Thus, as the patent discloses, deploying a plurality of monitors includes installing and configuring a plurality of generic monitors with reusable modules that define each monitor's functionality, as well as the analysis hierarchy of the monitors as a group.

SRI's construction that deploying simply means "locating" misses the meaning of the term in this context. Deploying a computing component involves configuring its operation. Moreover, the step calls for *deploying a plurality* of monitors, not just a single monitor, which implies arranging the monitors strategically, such as in forming an analysis hierarchy.[20] "Locating" does not capture this notion of strategic arrangement that stems from the plain meaning of *deploying*.

---

[17] *Id.* at 11:12-20 (emphasis added).

[18] *Id.* at 11:26-32 (emphasis added).

[19] *Id.* at 8:31-34 (emphasis added).

[20] This is in accord with the plain meaning of deploy, which is often utilized in the military context to indicate the strategic formation of units: "**deploy**, *v.t.* **1**. *Mil.* to

SRI's construction should be rejected because it does not reflect the alleged invention described in the patents and does not capture the plain meaning of *deploying*. Defendants' construction, which is in accord with the patent specification and plain meaning of *deploying*, should be adopted.

3. "hierarchical monitor"/"hierarchically higher network monitor"

Term	Defendants' Construction	SRI's Construction
hierarchical monitor / hierarchically higher network monitor	a *network monitor* that receives reports as input from one or more network monitors that are at a lower layer in the analysis hierarchy.	process or component in a network that receives reports from at least one lower-level monitor.

These constructions belie SRI's position that "the claims clearly establish" that network monitors are different components from hierarchical monitors.[21] The claims are explicit that a *hierarchical monitor* is a type of *network monitor*, which SRI implicitly concedes by proposing the same construction for the terms *hierarchical monitor* and *hierarchically higher network monitor*.

Rather than explain the contradictions raised in its constructions, SRI attempts to create diversions with its incorrect arguments relating to the opinions of Defendants' experts. SRI argues that the statements of Defendants' experts that require hierarchical

---

spread out (troops) so as to form an extended front or line. **2.** to arrange in a position of readiness, or to move strategically or appropriately: *to deploy a battery of new missiles.* - *v.i.* **3.** to spread out strategically or in an extended front or line. **4.** to come into a position ready for use: *the plane can't land unless the landing gear deploys.*" RANDOM HOUSE DICTIONARY OF THE ENGLISH LANGUAGE (Unabridged 2d ed. 1987) [Godfrey Decl., Ex. G]; *see also* WEBSTER'S II NEW COLLEGE DICTIONARY (1995) ("**deploy - ployed, -ploying, -ploys.** 1. To station (person or forces) systematically over an area, 2. To spread out (troops) to form an extended front.") [Godfrey Decl., Ex. H].

[21] SRI's Br. at 13-14 [D.I. 265].

monitors to generate reports are somehow inconsistent with Defendants' constructions.[22] There is no inconsistency. As shown in the attached claim chart,[23] all monitors, including hierarchical monitors, generate reports, as specified in '203 claim 1[c]. Even under SRI's constructions, hierarchical monitors generate "functional units," which SRI's expert identified as meta-reports. Thus, SRI's argument here is a red herring.

Finally, SRI incorrectly argues that Defendants' constructions result in a network monitor being the same thing as a hierarchical monitor.[24] Under Defendants' constructions, hierarchical monitors belong to the general class of network monitors, but they are distinguished by their position in the analysis hierarchy. As the claims specify and in accord with the plain meaning of the adjective "hierarchical," a hierarchical monitor also must be configured to receive reports from one or more network monitors that are at a lower layer in the analysis hierarchy. This construction is consistent with the claim language, specification and extrinsic evidence, and, therefore, should be adopted.

4. "service monitor"/"domain monitor"/"enterprise monitor"

Term	Defendants' Construction	SRI's Construction
service monitor	a *network monitor* that provides local real-time analysis of network packets handled by a network entity.	SRI does not believe the term needs construction but, if construed, should be construed to mean a network monitor that analyzes data from individual components or services.
domain monitor	a *network monitor* that receives and analyzes intrusion reports disseminated by *service monitors*.	SRI does not believe the term needs construction but, if construed, should be construed to mean a network monitor that analyzes data from a domain.

[22] *Id.* at 12-13.

[23] Godfrey Decl., Ex. B.

[24] SRI's Br. at 13-14 [D.I. 265].

enterprise monitor	a *network monitor* that receives and analyzes intrusion reports disseminated by *domain monitors*.	SRI does not believe the term needs construction but, if construed, should be construed to mean a network monitor that analyzes data from an enterprise, *i.e.* a collection of domains.

Service monitor, domain monitor and enterprise monitor are not terms of art, they are terms defined in the specification via the preferred embodiment. They have no meaning outside of that context. Defendants' proposed constructions reflect those definitions, which are used consistently throughout the specification.

SRI asserts that these terms have a "plain English-language meaning."[25] But SRI does not cite any dictionary definitions or other extrinsic evidence in support of its position. Nor does SRI specify what the purported "plain English-language meaning" is for these terms. Although SRI cites to the part of the patent stating "[e]ach domain 12a-12c includes one or more computers offering local and network services,"[26] it is unclear how this quote supports SRI's argument.

The constructions that SRI does offer are contrary to the specification and are ambiguous. Under SRI's construction, a *service monitor* could be solely a hierarchical monitor because, according to SRI, a *service monitor* analyzes "data from individual components." A "component" could be another monitor under SRI's constructions. Thus, a *service monitor* could be a network monitor that analyzes reports from other monitors; *i.e.,* a *hierarchical monitor*. Such a result is contrary to the specification's definition of a *service monitor* as a monitor at the lowest-level in the analysis hierarchy:

[25] SRI's Br. at 22, 25 [D.I. 265].

[26] '338 patent at 3:17-24 [D.I. 268, Ex. C].

"Service monitors 16a-16c provide local real-time analysis of network packets (e.g., TCP/IP packets) handled by a network entity 14a-14c."[27]

SRI's constructions of *domain* and *enterprise monitor* are similarly ambiguous. They call for analyzing "data from a domain" and "data from an enterprise," but what types of data are encompassed is unclear. SRI's constructions thus render the scope of the claims indefinite.

SRI argues that nothing in the claims or specification requires that *domain monitors* analyze reports from service monitors and that *enterprise monitors* analyze reports from *domain monitors*.[28] That assertion is demonstrably wrong. The specification states:

- "Domain monitors 16d-16e correlate intrusion reports disseminated by individual service monitors 16a-16c, providing a domain-wide perspective of activity (or patterns of activity)."[29]
- "Enterprise monitors 16f correlate activity reports produced across the set of monitored domains 12a-12c. . . . Enterprise 10 surveillance is very similar to domain 12a-12c surveillance: an enterprise monitor 16f subscribes to various domain monitors 16d-16e, just as the domain monitors 16d-16e subscribed to various service monitors 16a-16c."[30]

Similarly, the claims calling for domain and enterprise monitors depend from the step of "receiving and integrating" the reports.[31] Claim 10 of the '212 patent requires that the "receiving and integrating" be performed by "a domain monitor with respect to a plurality of service monitors." '212 claim 12 requires that the "receiving and integrating"

---

[27] *Id.* at 3:42-44.

[28] SRI's Br. at 23-25 [D.I. 265].

[29] '338 patent at 3:66-4:3 [D.I. 268, Ex. C].

[30] *Id.* at 4:19-31.

[31] *See* '212 claims 10 and 12 [D.I. 268, Ex. D].

be performed by "an enterprise monitor with respect to a plurality of domain monitors." Thus, the claim language is clear that a *domain monitor* analyzes reports from service monitors and that an *enterprise monitor* analyzes reports from domain monitors.

SRI's arguments and constructions here provide yet another illustration of the problems inherent in its inconsistent monitor construction. SRI argues that *hierarchical monitors* are not *network monitors*. Yet, SRI proposes constructions of *domain* and *enterprise monitors*—examples of *hierarchical monitors*—that specifically state they are *network monitors*. Rather than provide clarity for the members of the jury, SRI's constructions will have them running in circles. SRI's constructions should therefore be rejected.

5. "peer-to-peer relationships"

Term	Defendants' Construction	SRI's Construction
peer-to-peer relationships	relationship where entities at the same layer in a hierarchy receive reports from one another.	SRI does not believe the term needs construction but, if construed, should be construed to mean relationships between two or more entities at the same level in a hierarchy.

Defendants' construction results from the specification and the claims. Claim 11 of the '203 patent is representative of where this limitation appears in the claims: "the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another." As the patent states, this means that the domain monitors share reports: "Where mutual trust among domains 12a-12c exists, domain monitors 16d-16e may establish peer relationships with one another. Peer-to-peer

subscription allows domain monitors 16d-16e to share analysis reports produced in other domains 12a-12c."[32]

Defendants' construction is preferable because it explains what a peer-to-peer relationship means in the context of the patents-in-suit—sharing reports among monitors at the same level in the analysis hierarchy. SRI's construction fails to clarify what the peer-to-peer relationship entails and should therefore be rejected.

6. "hierarchical event monitoring and analysis"

Term	Defendants' Construction	SRI's Construction
hierarchical event monitoring and analysis	monitoring and analyzing events through the use of network monitors that are configured to form an analysis hierarchy of two or more layers.	monitoring events through the use of a hierarchical monitor.

In the context of the patents, and as reflected in Defendants' constructions, the method of *hierarchical event monitoring and analysis* is performed through the use of network monitors configured to form an analysis hierarchy. SRI's construction does little more than repeat the preamble and therefore provides no more context than the preamble itself. Thus, Defendants' constructions, which will help the jury understand the claims, should be adopted.

7. "selected from one or more"/"selected from"

Term	Defendants' Construction	SRI's Construction
based on analysis of network traffic data *selected from* one or more of the following categories… based on analysis of network traffic data *selected from* the following categories…	analysis is based on one or more of the following categories.	SRI does not believe the phrase needs construction.

[32] '338 patent at 4:8-12 [D.I. 268, Ex. C].

Defendants offer constructions for these terms to make it clear to the jury that even though the '203 and '615 patents use slightly different language—"selected from one or more of the following" versus "selected from the following"—these claim terms mean the same thing. Since SRI does not dispute the accuracy of the construction, and Defendants believe it will assist the jury, there is no reason not to adopt the construction.

8. "integrating"/"correlating"

Term	Defendants' Construction	SRI's Construction
automatically receiving and *integrating* the reports of suspicious activity, [by one or more hierarchical monitors]	automatically receiving and combining the reports of detected suspicious network activity.	without user intervention, receiving reports and combining those reports into another functional unit.
[Dependent claims:] wherein integrating comprises *correlating* intrusion reports reflecting underlying commonalities	determining relationships among the reports of detected suspicious network activity.	combining the reports based on underlying commonalities between them.

SRI's constructions are similar to Defendants' constructions, except that SRI unnecessarily attempts to limit the scope of these terms to avoid the prior art.

First, the plain and ordinary meaning of *automatically* is broader than "without user intervention." As reflected in the dictionary definitions provided by SRI, automatically means "[a]cting or operating in a manner *essentially independent* of external influence or control."[33] This definition recognizes that there may be some limited user intervention. Most, if not all, automated components need to be configured at some point by a user. SRI's construction of "without user intervention" appears to

[33] SRI's Br. at 15 [D.I. 265].

preclude this. There is no support in the patents, or in the cited dictionary definitions, for limiting the well-understood term *automatically* in the manner proposed by SRI. Thus, SRI's construction should be rejected.

SRI's construction of *integrate*, which requires "combining those reports into another functional unit," also creates ambiguity by introducing a vague new term—"functional unit"—without explaining its meaning. Nowhere do the patents use this term. Moreover, as discussed in Defendants' opening brief, SRI's expert testified that he viewed the term as requiring the generation of a meta-alert, a report on which further analysis could take place. But, since generating reports by *monitors* is already a claim element, there is no need to put that requirement in twice. Under Defendants' proper construction, the claim language is clear—all *monitors* generate reports, and the *integrating* step further specifies that a *hierarchical monitor*, in its analysis, is to combine reports generated by lower-level monitors.

In the patent claims, the term *correlating* always depends from *integrating* and therefore further limits it. Defendants' construction, which recognizes this context, properly defines *correlating* as determining relationships among the reports. The determined relationship indicates the underlying commonalities among the reports. In contrast, SRI's construction adds no clarity—"combining" is part of the step of *integrating* and "based on underlying commonalities" is specified in the claims.

SRI's constructions should be rejected as adding unnecessary limitations and ambiguity. Defendants' constructions, which clarify the language, should be adopted.

9. "responding"/"invoking countermeasures"

Term	Defendants' Construction	SRI's Construction
responding . . . / invoking countermeasures	taking an action in response to a suspected attack, including passive responses such as report dissemination to other monitors or administrators, and highly aggressive actions, such as severing a communication channel or the reconfiguration of logging facilities within network components.	taking an action in response.

Defendants offer a construction of these terms because the specification indicates a definition of *countermeasures* that includes passive responses, which is somewhat different than the ordinary meaning of *countermeasure*:

> "Countermeasures range from very passive responses, such as report dissemination to other monitors 16a-16f or administrators, to highly aggressive actions, such as severing a communication channel or the reconfiguration of logging facilities within network components (e.g., routers, firewalls, network services, audit daemons)."[34]

Because this definition is different from the ordinary meaning of countermeasures, Defendants believe that the full definition should be given to the Jury to avoid any confusion.

10. "proxy server"

Term	Defendants' Construction	SRI's Construction
proxy server	a firewall component that enforces a security policy for a specific application or service.	SRI does not believe the term needs construction but, if construed, should be construed to mean a server that mediates communication between a client application, such as a Web browser, and a real server. It handles requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.

[34] '338 patent at 12:7-12 [D.I. 268, Ex. C].

The reason this term needs construction is that SRI fails to use the definition of proxy server *from the relevant time frame*. In the 1997-1998 timeframe, *proxy servers* were understood to be a firewall component:

> "**proxy server ...** *n.* A firewall component that manages Internet traffic to and from a local area network (LAN) and can provide other features, such as document caching and access control."[35]

Even SRI's cited extrinsic evidence shows *proxy server* as part of a firewall component.[36]

As reflected in Defendants' construction, a proxy server at that time was a firewall component. It managed Internet traffic as part of a firewall component—i.e., it enforced a security policy with respect to traffic. It did that in its role as a *proxy*, a security control point between the real server and the client seeking access.[37] Because proxying works differently from service to service, it was not uncommon to have a different proxy service for each application or service.[38]

A *proxy server* is a specific component of a firewall that acts as a control point for a specific application or service. Firewall is a broader term. Thus, contrary to SRI's assertions, '615 claim 64, which specifies that at least one monitor is deployed at a firewall, is distinct from '615 claim 54, which is exactly the same except that it specifies that a monitor is deployed at a *proxy server*.

Defendants' construction of *proxy server* as "a firewall component that enforces a

---

[35] COMPUTER DICTIONARY, Microsoft Press (3d ed. 1997) [Godfrey Decl., Ex. I].

[36] *See* Declaration of Kyle Wagner Compton, Ex. M [D.I. 266].

[37] D. Brent Chapman & Elizabeth D. Zwicky, BUILDING INTERNET FIREWALLS 190-91 (1995) (SYM_P_0498540-41) [Godfrey Decl., Ex. J].

[38] *See id.* at 192-93 (SYM_P_0498542-43).

security policy for a specific application or service" is reflective of how that term would have been understood at the time the patent was filed. SRI's construction, which fails to indicate that a *proxy server* was a firewall component is not, and therefore should be rejected.

11. "API"

Term	Defendants' Construction	SRI's Construction
API	standard interface specification for communication.	a set of routines used to provide for communication of data between application programs or processes.

The parties did not address this term in their Joint Claim Construction Statement because it is a well-known term of art. SRI belatedly attempted to offer a construction for this term in its opening claim construction brief. In case the Court were to construe this term, Defendants offer their own proposal, which defines the term consistently with the specification and the plain meaning.

A representative claim using this term is claim 4 of the '203 patent:

> **4.** The method of claim 1, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.

As the specification explains, the API of the network monitors is a "*standard interface specification for communication* within and between monitor elements and external modules."[39] As reflected in the claims, and further discussed in the specification, this standard communication interface allows modules within a monitor to communicate, which in turns allows for "encapsulation of monitor functions." It also allows for third-

[39] '338 patent at 9:8-11 (emphasis added) [D.I. 268, Ex. C].

party tools to communicate with the network monitors of the claims via the standard communication interface defined for the monitor.

This use of API is consistent with its plain meaning in the art at the time of filing:

> **application program interface** A series of defined interface standards for an application. An API typically defines how an application should appear to a user, how input should be requested and obtained, and how output should be done.[40]

Thus, Defendants' construction is in accord with the patent specification and plain meaning of the term API.

SRI's construction misses the point of providing a *standardized interface* for an API that allows for both encapsulation of monitor functions and integration of third-party tools. In addition, SRI's construction adds unnecessary complexity that a jury may have a hard time understanding. Any standardized interface implies that there are routines used to provide the communication in accordance with that standard. The real issue for the jury to understand is that an API is a standardized interface for communication.

[40] COMPUTER PROFESSIONAL'S DICTIONARY (1990) [Godfrey Decl., Ex. K].

B. Statistical Detection Claims

1. "building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets"

Term	Defendants' Construction	SRI's Construction
building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets	"automatically generating and updating an exponentially aged probability distribution of historically observed activities from at least one measure of the network packets" "automatically generating and updating an exponentially aged probability distribution of recently observed activities from at least one measure of the network packets"	"creating at least one statistical description representative of historical network activity, and creating at least one statistical description of recent network activity, where the descriptions are based on one or more measures of network packets"

The parties agree that, as described in the specification, a long-term statistical profile is based on historically observed network activities and a short-term statistical profile is based on recently observed network activities.[42] But the parties disagree about whether the remainder of this claim language should likewise be construed to reflect the specification's disclosure regarding statistical profiling.

One difference between the proposed constructions is that Defendants construe "building" to mean "automatically generating and updating," whereas SRI construes this term to mean "creating." SRI argues that "building" seems "pretty straightforward," and that "[i]t is also not apparent where Defendants' 'generating and updating' language comes from."[43] In fact, Defendants' language comes directly from the specification,[44]

---

[41] Defendants believe it is easier to understand this limitation if the long-term and short-term statistical profiles are addressed separately. However, this is not a major substantive difference between the parties.

[42] *See* SRI's Br. at 18-19 [D.I. 265]; Defendants' Br. at 30-35 [D.I. 267].

[43] SRI's Br. at 20 [D.I. 265].

which is the same place SRI's language comes from.[45]

Nothing turns on the choice of "generating" versus "creating" to explain the claim term "building." The problem with SRI's proposed construction is that it fails to account for the specification's disclosure that the claimed statistical profiles are updated, and that the initial building and subsequent updating of the statistical profiles is performed automatically (i.e., by a network monitor, not by a human).[46] These two requirements are essential. If the claimed statistical profiles are not automatically updated, the long-term statistical profile cannot represent "normal" activity,[47] the short-term statistical profile cannot be "cleared" at "update time,"[48] and a network monitor cannot compare the profiles to achieve the advantage touted in the specification of detecting abnormal activity "without requiring an administrator to catalog each possible attack upon a network"[49] and "without burdening a network administrator with the task of arbitrarily setting an unvarying threshold."[50] *Cf. Toro Co. v. White Consolidated Indus., Inc.*, 199 F.3d 1295, 1300-02 (Fed. Cir. 1999) (construing term "cover *including* [a restriction

---

[44] *See, e.g.*, '338 patent at 14:7-8 ("A long-term and short-term statistical profile can be generated for each event stream."), 6:38-41 ("The system maintains and updates a description of behavior with respect to these measure types in an updated profile. The profile is subdivided into short-term and long-term-profiles.") [D.I. 268, Ex. C]

[45] *See id.* at 14:35-36 ("By creating and updating short-term statistical profiles . . . .").

[46] *See, e.g., id.* at 6:38-50, 14:26-30; Phillip A. Porras & Alfonso Valdes, *Live Traffic Analysis of TCP/IP Gateways*, 1998 ISOC Symposium on Network and Distrib. Sys. Sec., at 4 ("*Live Traffic Analysis* paper") [D.I. 268, Ex. O].

[47] '338 patent at 2:46 [D.I. 268, Ex. C].

[48] *Id.* at 6:47-50.

[49] *Id.* at 2:46-48; *see also id.* at 6:57-58 ("Furthermore, the algorithms require no a priori knowledge of intrusive or exceptional activity."); Valdes Tr. 135:1-11 (REDACTED Godfrey Decl., Ex. E].

[50] '338 patent at 13:22-27 [D.I. 268, Ex. C].

ring]" to require that the restriction ring be "permanently affixed" to the cover, because this was the only embodiment disclosed in the specification and the specification described this unitary structure as advantageous).

A second difference between the proposed constructions is that Defendants construe "statistical profile" to mean an "exponentially aged probability distribution," whereas SRI construes this term to mean a "statistical description." SRI incorrectly argues that "[n]othing in the . . . specification requires or suggests such limitations."[51] In fact, the specification expressly teaches that the claimed statistical profiles are exponentially aged:

> ***The short-term profile*** accumulates values between updates, and ***exponentially ages*** (e.g., weighs data based on how long ago the data was collected) values for comparison to the long-term profile. As a consequence of the aging mechanism, the short-term profile characterizes recent activity, where "recent" is determined by a dynamically configured aging parameters. At update time (typically, a time of low system activity), the update function folds the short-term values observed since the last update into the long term profile, and the short-term profile is cleared. ***The long-term profile is itself slowly aged*** to adapt to changes in subject activity.[52]

The *Statistical Methods* paper, which is co-authored by one of the inventors and incorporated by reference into the specification,[53] also states that the long-term and short-term statistical profiles are exponentially aged:

> The fading memory concept is implemented by ***exponential aging*** . . . . Updating consists of ***exponential fading*** of the existing long-term profile . . . . ***Exponential fading of both profiles*** (using different time constants) permits relatively compact representation of the profiles as well as a mechanism for forgetting activity from the distant past not repeated in the recent past. ***Exponential fading*** of the short-term profile takes place as

---

[51] SRI's Br. at 19 [D.I. 265].

[52] '338 patent at 6:42-52 (emphasis added) [D.I. 268, Ex. C].

[53] *Id.* at 5:42-48.

> each audit record is received, while fading of the long-term profile takes place at profile update time.[54]

Publications incorporated by reference to explain the claimed invention are "highly relevant to one of ordinary skill in the art for ascertaining the breadth of the claim term." *AquaTex Indus., Inc. v. Techniche Solutions*, 419 F.3d 1374, 1381 (Fed. Cir. 2005); *see also V-Formation, Inc. v. Benetton Group SpA*, 401 F.3d 1307, 1311 (Fed. Cir. 2005) ("This court has established that prior art cited in a patent or cited in the prosecution history of the patent constitutes intrinsic evidence. . . . when prior art that sheds light on the meaning of a term is cited by the patentee, it can have particular value as a guide to the proper construction of the term, because it may indicate not only the meaning of the term to persons skilled in the art, but also that the patentee intended to adopt that meaning.") (internal quotations omitted); *L.G. Philips LCD Co. v. Tatung Co.*, 2006 U.S. Dist. LEXIS 38942, at *8 n.1 (D. Del. 2006) (narrowly construing disputed claim term consistent with its use throughout the specification, including in publication incorporated by reference); *Sunny Fresh Foods, Inc. v. Michael Foods, Inc.*, 205 F. Supp. 2d 1077, 1092 (D. Minn. 2002) (same).

SRI dismisses "exponential aging" as merely a characteristic of a preferred embodiment.[55] But SRI's reasoning is flawed. First, SRI suggests that the specification's reference to "configur[able] aging parameters"[56] indicates that that the profile aging

---

[54] Alfonso Valdes & Debra Anderson, *Statistical Methods for Computer Usage Anomaly Detection Using NIDES*, Proceedings of the Third Int'l Workshop on Rough Sets and Soft Computing (Jan. 1995), at 306-07 ("*Statistical Methods* paper") (emphasis added) [D.I. 268, Ex. N].

[55] SRI's Br. at 19-20 [D.I. 265].

[56] *See* '338 patent at 6:42-47 [D.I. 268, Ex. C]; *Live Traffic Analysis* paper at 4 [D.I. 268, Ex. O].

mechanism can be configured so that there is no exponential aging.[57] The specification teaches no such thing. Rather, the cited passage teaches that the ***rate*** of exponential aging (and therefore the effective lifespan of data within a profile) can be configured. The incorporated *Statistical Methods* paper explains this concept by noting that the short-term and long-term statistical profiles are exponentially aged "using different time constants."[58]

Next, SRI notes that part of the specification discusses the claimed statistical profiles "without any reference to aging at all."[59] But the passage cited by SRI is the "Summary" of the invention section of the specification, which, in SRI's patents, does little more than recite the claim language. This "Summary" does not disclose any embodiments different from the ones disclosed in the "Detailed Description" section.

Here, the specification and the inventors' incorporated publications do not disclose any alternative for accounting for the life span of collected data other than by exponentially aging that data.[60] Moreover, the specification describes the "exponential aging" requirement in absolute terms, without using language such as "embodiments may include" or "for example," as is used elsewhere in the specification to identify preferred

---

[57] SRI's Br. at 19-20 [D.I. 265].

[58] *Statistical Methods* paper at 307 [D.I. 268, Ex. N].

[59] SRI's Br. at 19-20 (citing '338 patent at 1:44-2:53) [D.I. 265].

[60] *See, e.g.*, Valdes Tr. 371:6-8 [Godfrey Decl., Ex. E]; Kesidis Tr. 436:18-437:4 REDACTED

REDACTED 438:1-25 [Godfrey Decl., Ex. D].

embodiments.[61] *Cf. L.G. Philips*, 2006 U.S. Dist. LEXIS 38942, at *16 n.3 ("The Court also notes that the patentee explicitly stated that certain elements of the invention could vary from the specific descriptions in that embodiment, but did not include the [disputed claim term] among those elements."). Exponential aging of the statistical profiles "is not simply the preferred embodiment; it is the only embodiment." *Toro Co.*, 199 F.3d at 1301.

"Although claims need not be limited to the preferred embodiment when the invention is more broadly described, neither do the claims enlarge what is patented beyond what the inventor has described as the invention." *Inpro II Licensing, S.A.R.L. v. T-Mobile USA, Inc.*, 2006 U.S. App. LEXIS 11675, at *10 (Fed. Cir. 2006) (internal quotation omitted); *see also Lizardtech v. Earth Res. Mapping, Inc.*, 433 F.3d 1373, 1375 (Fed. Cir. 2006) ("[I]n whatever form the claims are finally issued, they must be interpreted, in light of the written description, but not beyond it, because otherwise they would be interpreted to cover inventions or aspects of an invention that have not been disclosed. Claims are not necessarily limited to preferred embodiments, but, if there are no other embodiments, and no other disclosure, then they may be so limited."). Thus, in similar cases, the Federal Circuit and this Court have construed facially broad claim language more narrowly to account for the rest of the intrinsic record. *See Network Commerce, Inc. v. Microsoft Corp.*, 422 F.3d 1353, 1358-61 (Fed. Cir. 2005); *Warner-Lambert Co. v. Schwarz Pharma, Inc.*, 418 F.3d 1326, 1340 (Fed. Cir. 2005); *Toro Co.*, 199 F.3d at 1300-02; *L.G. Philips*, 2006 U.S. Dist. LEXIS 38942, at *6-8.

[61] *See, e.g.*, '338 patent at 1:55, 7:50 [D.I. 268, Ex. C].

SRI also takes issue with Defendants' description of a statistical profile as a "probability distribution," noting that this term "does not even appear in the specification."[62] But in the incorporated *Statistical Methods* paper, one of the inventors uses this very term to describe both short-term and long-term statistical profiles:

> For each measure, we construct a ***probability distribution*** of short-term and long-term behaviors. For example, for the measure of file access, the ***long-term probability distribution*** would consist of the historical probabilities with which different files have been accessed, and the ***short-term probability distribution*** would consist of the recent probabilities with which different files have been accessed.[63]

And SRI's expert, Dr. Kesidis, agreed that one of ordinary skill in the art would have understood the term "statistical profile" to reflect a probability distribution.[64] By contrast, SRI's proposed construction—"statistical description"—does not appear anywhere in the specification, not even in the inventors' publications which are incorporated by reference. Nor does it explain what "statistical" means in this context. *Cf. Harris Corp. v. IXYS Corp.*, 114 F.3d 1149, 1152 (Fed. Cir. 1997) (rejecting a proposed construction on the grounds that it was circular). SRI asserts that its proposed construction "conveys the plain meaning of the claim terms."[65] But SRI cites no

---

[62] SRI's Br. at 19 [D.I. 265].

[63] *Statistical Methods* paper at 307 (emphasis added) [D.I. 268, Ex. N]; *cf.* Valdes Tr. 196:7-12

REDACTED

[Godfrey Decl., Ex. E].

[64] *See* Kesidis Tr. 440:1-7, 439:1-8 [Godfrey Decl., Ex. D].

[65] SRI's Br. 19-20 [D.I. 265].

evidence, extrinsic or otherwise, to support its contention that the term "statistical profile" had an inherent meaning to one of ordinary skill in the art as of 1998.

Defendants' proposed construction should be adopted because it provides a more specific and meaningful explanation of the disputed claim term, and accounts for the inventors' consistent use of that term throughout the entire intrinsic record.

2. "determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious activity"

Term	Defendants' Construction	SRI's Construction
determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious activity	determining whether the difference between the *short-term statistical profile* and *long-term statistical profile* exceeds a threshold that is empirically determined to indicate suspicious activity based on the historically adaptive deviation between the two profiles, requiring no prior knowledge of suspicious activity.	SRI does not believe the term needs construction but, if construed, should be construed to mean using the result of the comparison to decide whether the monitored activity is suspicious.

SRI's proposed construction for this term is overly broad and does not account for the specific disclosure in the specification regarding ***how*** a network monitor determines whether the difference between the statistical profiles indicates suspicious activity.[66]

The specification teaches that anomalous (i.e., suspicious) network activity is identified by calculating the degree of difference between corresponding values in the short-term and long-term statistical profiles and then determining whether that difference exceeds a historically adaptive difference:

> The distribution of recently observed values is compared against the long-term profile, and a distance between the two is obtained. The difference is

[66] Moreover, the SRI construction leaves the step indefinite because it fails to indicate the scope of what activity will be deemed "suspicious activity," or even how such a decision is to be made.

> compared to a historically adaptive deviation. The empirical distribution of this deviation is transformed to obtain a score for the event. Anomalous events are those whose scores exceed a historically adaptive score threshold based on the empirical score distribution.[67]

The specification also teaches that this statistical anomaly detection approach requires no prior knowledge of what constitutes suspicious network activity: "The algorithms require no a priori knowledge of intrusive or exceptional activity."[68]

SRI argues that this language must describe a preferred embodiment because "the specification also describes comparisons between long-term and short-term profiles that do not require these limitations."[69] What SRI again fails to mention is that the passage it cited is from the "Summary" section of the specification. This "Summary" does not disclose different embodiments having different features from those embodiments disclosed in the "Detailed Description" section.

Here, the specification discloses a single method, quoted above, for how to determine whether the difference between a short-term and a long-term statistical profile indicates suspicious network activity. This method is described in absolute terms,

---

[67] '338 patent at 6:60-67 [D.I. 268, Ex. C]; *see also Statistical Methods* paper at 308-09 [D.I. 268, Ex. N]; Valdes Tr. 131:16-132:1, 133:9-134:24 [Godfrey Decl., Ex. E]; Kesidis Tr. 62:5-17, 74:22-78:8, 186:21-187:21, 281:4-282:7 [Godfrey Decl., Ex. D].

[68] '338 patent at 6:57-58 [D.I. 268, Ex. C]; *see also Live Traffic Analysis* paper at 4 (same) [D.I. 268, Ex. O]; '338 patent at 2:46-48 ("As long-term profiles represent 'normal' activity, abnormal activity may be detected without requiring an administrator to catalog each possible attack upon a network."), 7:5-8 ("The mathematical functions for anomaly scoring, profile maintenance, and updating do not require knowledge of the data being analyzed beyond what is encoded in the profile class.") [D.I. 268, Ex. C]; *Statistical Methods* paper at 306 ("The NIDES statistical approach requires no *a priori* knowledge about what types of behavior would result in compromised security. It simply compares short-term and long-term behaviors to determine whether they are statistically similar.") [D.I. 268, Ex. N]; Valdes Tr. 130:25-131:6, 135:1-11, 365:16-366:19 [Godfrey Decl., Ex. E]; *cf.* Kesidis Tr. 481:19-482:4 [Godfrey Decl., Ex. D].

[69] SRI's Br. at 28 (citing '338 patent at 1:44-2:53) [D.I. 265].

without using language such as "embodiments may include" or "for example," as is used elsewhere in the specification to identify preferred embodiments.[70] *See L.G. Philips*, 2006 U.S. Dist. LEXIS 38942, at *16 n.3. Use of this disclosed method is essential to the invention. For example, if the degree of difference between the long-term and short-term statistical profiles is not compared to a learned threshold that has been "empirically determined . . . based on the historically adaptive deviation between the two profiles," the statistical profiling approach will not achieve the advantage of identifying suspicious network activity without requiring prior knowledge of intrusive or exceptional activity.[71]

Defendants' proposed construction should be adopted because it accounts for the inventors' consistent use of the disputed term throughout the entire intrinsic record. *See Network Commerce*, 422 F.3d at 1358-61; *Warner-Lambert Co.*, 418 F.3d at 1340; *Toro Co.*, 199 F.3d at 1300-02; *L.G. Philips*, 2006 U.S. Dist. LEXIS 38942, at *6-8.

---

[70] *See, e.g.*, '338 patent at 1:55, 7:50 [D.I. 268, Ex. C].

[71] *See id.* at 6:57-58; *see also Statistical Methods* paper at 308 ("The degree of difference between the long-term profile for a measure and the short-term profile of a measure is quantified . . . . We call the resultant numerical value Q . . . . Unfortunately, it is not possible to refer Q directly to a chi-square table due to potential dependence and insufficient observations for some bins in the data stream on which Q is based. Since the distribution of Q is not chi-squared, we need to track its values to determine what its distribution looks like. We observe the values for Q . . . and build an empirical probability distribution for Q using an aging and updating mechanism similar to that used for the measure categories. There is a Q statistic and a corresponding Q distribution for each measure.") [D.I. 268, Ex. N]; *cf.* Valdes Tr. 135:1-11 REDACTED Godfrey Decl., Ex. E].

REDACTED

3. "a statistical detection method"

Term	Defendants' Construction	SRI's Construction
a statistical detection method	a method of detecting suspicious network activity which comprises building a *long-term statistical profile* and a *short-term statistical profile*. This method requires no prior knowledge of suspicious network activity. This method is not a signature matching detection method or threshold analysis.	SRI does not believe the term needs construction but, if construed, should be construed to mean a method of detecting suspicious network activity by applying one or more statistical functions in the analysis of network traffic data.

SRI's proposed construction for "a statistical detection method" should not be adopted because it is overly broad and circular.

SRI provides no support for its assertion that the words "statistical detection method" have "a plain English-language meaning," and that SRI's proposed construction "reflects the plain meaning of the term."[72] Deposition testimony from SRI's expert and both inventors indicates that this term had no clear inherent meaning to one of ordinary skill in the art as of November 1998.[73] One of ordinary skill in the art would therefore look to the intrinsic record, in particular the specification, to understand this claim term. *See Network Commerce*, 422 F.3d at 1359-60; *L.G. Philips*, 2006 U.S. Dist. LEXIS 38942, at *17.

SRI's proposed construction is overly broad because building and comparing long-term and short-term statistical profiles to identify statistical anomalies indicative of suspicious network activity is the only "statistical detection method" invention disclosed

[72] SRI's Br. at 29-30 [D.I. 265].

[73] *See* Defendants' Br. at 38 (discussing relevant deposition testimony) [D.I. 267].

in the specification.[74] "Although claims need not be limited to the preferred embodiment when the invention is more broadly described, neither do the claims enlarge what is patented beyond what the inventor has described as the invention." *Inpro II Licensing*, 2006 U.S. App. LEXIS 11675, at *10 (internal quotation omitted). SRI makes three arguments why "a statistical detection method" should be construed to encompass detection methods other than statistical profiling. Each of SRI's arguments is flawed.

First, SRI argues that use of the phrase "statistical detection method" instead of the statistical profiling language used in the '338 claims "demonstrates that the limitations are not the same."[75] But that is not the law. *See Inpro II Licensing*, 2006 U.S. App. LEXIS 11675, at *7 ("[D]escribing claim elements or limitations in different words does not invariably change the scope of the claim."); *Nystrom*, 424 F.3d at 1143 ("Different terms or phrases may be construed to cover the same subject matter where the written description and prosecution history indicate that such a reading of the terms or phrases is proper."); *Digital Biometrics, Inc. v. Identix, Inc.*, 149 F.3d 1335, 1347 (Fed. Cir. 1998) (rejecting Plaintiff's argument that, because different words were used in the other claims, the disputed claim term must have a unique (and broader) meaning). In the context of the shared specification, which discloses only one "statistical detection method," a more reasonable explanation is that the patentees used the phrase "statistical detection method" because it is shorter. *Cf. Beery v. Thomson Consumer Elecs., Inc.*, 2004 U.S. Dist. LEXIS 17173, at *43 (S.D. Ohio Aug. 18, 2004) ("[O]ne reason for permitting an inventor to act as his or her own lexicographer is to make claim language

[74] *See, e.g.*, '338 patent at 5:36-7:22 [D.I. 268, Ex. C]; Kesidis Tr. 189:22-190:9 [Godfrey Decl., Ex. D].

[75] SRI's Br. at 30 [D.I. 265].

more concise, and hence more easily understood."). Had the patentees' re-used claim language from the '338 patent, the hierarchical monitoring claims, which include a number of additional limitations, would have been unwieldy. For example, '212 claim 1 would have read:

> Method for monitoring an enterprise network, said method comprising the steps of:
> deploying a plurality on network monitors in the enterprise network;
> detecting, by the network monitors, suspicious network activity based on analysis on network traffic data, wherein at least one of the network monitors utilizes *[A method of network surveillance, comprising:*
> *receiving network packets handled by a network entity;*
> *building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets, the at least one measure monitoring data transfers, errors, or network connections;*
> *comparing at least one long-term and at least one short-term statistical profile; and*
> *determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity]*;
> generating, by the monitors, reports of said suspicious activity; and
> automatically receiving and integrating the reports of suspicious network activity, by one or more hierarchical monitors.

The patentees avoided this problem by using "a statistical detection method" as shorthand for the one and only statistical detection method addressed in the patents-in-suit.

Second, SRI argues that the specification discloses statistical detection methods other than the one comprising building and comparing long-term and short-term statistical profiles: "The specification is similarly broad, describing statistical techniques involving categorical approaches and analysis of network connection information without requiring that they necessarily use long-term profiles."[76] But the paragraph cited by SRI

[76] SRI's Br. at 29 (citing '338 patent at 13:27-49) [D.I. 265].

does not disclose any other statistical detection methods. It discloses different "measures" of network traffic from which the long-term and short-term statistical profiles can be built. This is evident when the passage cited by SRI is read in context.

In particular, the relevant section begins at column 12, line 46, with reference to Fig. 4 of the patents-in-suit. Fig. 4 discloses that a monitor performs "network surveillance" by "build[ing] statistical profiles from measures derived from network packets."[77] ("Network surveillance" is the title of the '338 and '212 patents, and is the term used in the "Summary" of the invention section to describe the statistical profiling detection method.[78]) After this initial paragraph summarizing the statistical profiling method, the specification states: "A few examples can illustrate ***this method of network surveillance***."[79] The passage cited by SRI provides some of these examples of the statistical profiling method of network surveillance applied to different measures of network traffic; it does not teach other statistical detection methods. In fact, neither inventor could identify any statistical detection methods other than the statistical profiling method disclosed in the specification.[80]

Third, SRI argues that one can infer from the absence of any substantive prosecution history that the examiner believed the claim term "statistical detection method" was different in scope from the statistical profiling method disclosed in the

---

[77] '338 patent at 3:8 and Fig. 4 [D.I. 268, Ex. C].

[78] *See id.* at 1:44-45, 2:11-12, 2:36-37.

[79] *Id.* at 12:66-67 (emphasis added).

[80] *See* Valdes Tr. at 377:17-379:12 [Godfrey Decl., Ex. E]; Porras Tr. 141:16-142:5 [Godfrey Decl., Ex. F].

specification and claimed in the '338 patent: "Indeed, if the Examiner believed these limitations were the same, one would have expected a double-patenting rejection or, at the very least, some statement in the prosecution questioning the use of different terminology if the intent was to claim the same subject matter."[81] No such inference is warranted. The claims which use the "statistical detection method" language contain many additional hierarchical architecture limitations which distinguish them in scope from the '338 claims.[82] Thus, there was no basis for a double-patenting rejection, or any other statement questioning the patentees' use of the "statistical detection method" phrase in the '212 claims and '615 claim 7. *See generally* MPEP § 803 ("Definition of Double Patenting").

Another reason SRI's proposed construction should not be adopted is because it defines "statistical detection method" in a circular manner using the phrase "statistical functions," without explaining what "statistical" means in the context of the patents-in-suit. *See Harris Corp.*, 114 F.3d at 1152 (rejecting a proposed construction on the grounds that it was circular). In its opening claim construction brief, SRI acknowledged that one of the objectives of claim construction is "to clarify and when necessary to explain what the patentee covered by the claims."[83] But the ambiguity in SRI's proposed construction of "statistical detection method" provides little guidance when evaluating possible infringement. For example, the patents-in-suit distinguish between "statistical"

---

[81] SRI's Br. at 30 [D.I. 265].

[82] *Compare* '212 claim 1 [D.I. 268, Ex. D] *with* '338 claim 1 [D.I. 268, Ex. C].

[83] SRI's Br. at 4 (quoting *United States Surgical Corp. v. Ethicon, Inc.*, 103 F.3d 1554, 1568 (Fed. Cir. 1997)) [D.I. 265].

and "signature" detection methods.[84] But if "statistical functions" includes simple mathematical operations, such as counting the number of occurrences of an event,[85] then SRI's proposed construction would encompass forms of threshold analysis which the patents (and SRI's expert) define as a "rudimentary, inexpensive ***signature*** analysis technique," not the claimed "statistical detection method."[86] Thus, SRI's construction cannot be correct.

Defendants' proposed construction should be adopted because it accounts for the entire intrinsic record, including the patents' distinction between "signature" detection methods and the claimed "statistical detection method." *See Network Commerce*, 422 F.3d at 1358-61; *Warner-Lambert Co.*, 418 F.3d at 1340; *Toro Co.*, 199 F.3d at 1300-02; *L.G. Philips*, 2006 U.S. Dist. LEXIS 38942, at *6-8.

4. "a signature matching detection method"

Claim Term	Defendants' Construction	SRI's Construction
a signature matching detection method	a method of detecting suspicious activity which comprises comparing observed network traffic data to known patterns or thresholds.	SRI does not believe the term needs construction but, if construed, should be construed to mean a method of detecting suspicious network activity by comparing observed network traffic data to known patterns.

[84] *See, e.g.*, '212 claim 3 ("The method of claim 2, wherein the monitor utilizing a signature matching detection method also utilizes a statistical detection method.") [D.I. 268, Ex. D].

[85] *See, e.g.*, Microsoft Office Online Assistance Guide for Excel 2003, at http://office.microsoft.com/en-us/assistance/HP052030661033.aspx (listing counting ("COUNT") as a "statistical function") [Godfrey Decl., Ex. L]; Valdes Tr. 106:9-17 [Godfrey Decl., Ex. E].

REDACTED

[86] '338 patent at 7:45-53 (emphasis added) [D.I. 268, Ex. C]; *see also Live Traffic Analysis* paper at 8 [D.I. 268, Ex. O]; Kesidis Tr. 483:3-484:1, 487:3-490:10, 493:12-494:13, 501:18-502:20 [Godfrey Decl., Ex. D].

The parties' proposed constructions for this term are very similar. Both constructions include the phrase, "a method of detecting suspicious network activity," to account for the specification's disclosure that signature matching techniques can be used to detect not just known attacks, but also suspicious activity that might represent an attack or investigation to facilitate future attacks.[87] Both proposed constructions also reflect the specification's disclosure that signature detection methods involve comparing network traffic data to known patterns.[88]

The only difference between the parties' proposed constructions is that Defendants' construction expressly recites a particular example of a "signature matching detection method"—matching observed network traffic data to *known thresholds*. This example is consistent with the specification, which defines "threshold analysis" (i.e., use of a preset, fixed threshold as a point of comparison to identify suspicious network activity) as an example of a signature matching detection method:

> Threshold analysis is a rudimentary, inexpensive signature analysis technique that records the occurrence of specific events and, as the name implies, detects when the number of occurrences of that event surpasses a reasonable count. For example, monitors can encode thresholds to monitor activity such as the number of fingers, pings, or failed login requests to accounts such as guest, demo, visitor, anonymous FTP, or employees who have departed the company.[89]

---

[87] *See* '338 patent at 7:23-8:13 [D.I. 268, Ex. C]; SRI's Br. at 32 [D.I. 265].

[88] *See* '338 patent at 7:23-26 [D.I. 268, Ex. C]; *Live Traffic Analysis* paper at 7-8 [D.I. 268, Ex. O].

[89] '338 patent at 7:45-53 [D.I. 268, Ex. C]; *see also id.* at 13:22-27 (distinguishing the statistical profiling detection method from detection methods that require a network administrator to set an "unvarying threshold"); *Live Traffic Analysis* paper at 6 (distinguishing the statistical profiling detection method from detection methods involving "user-definable heuristic rules that specify fixed thresholds"), 7-8 ("Signature analysis is a process whereby an event stream is mapped against abstract representations of event sequences known to indicate the target activity of interest. . . . For example, EMERALD surveillance modules can encode thresholds to monitor activity such as the number of fingers, pings, or failed login requests to accounts such as guest, demo, visitor,

SRI argues that this passage from the specification merely means that "thresholds *can be* used in 'rudimentary, inexpensive signature analysis.'"[90] But that is not what the specification says, nor what it teaches.[91]

SRI also argues that Defendants' proposed construction is overly broad because it treats "*all* use of thresholds in all contexts" as "signature matching."[92] But that too is a mischaracterization. Defendants' proposed construction does not cover any and all uses of a threshold to detect suspicious network activity; it covers "comparing observed network traffic data to known . . . thresholds." Defendants' proposed construction does not cover, for example, comparing the difference between two statistical profiles to a dynamic, subject-specific threshold that is learned by a network monitor (as is done in the statistical detection method disclosed in the patents),[93] because such a comparison does not involve matching *observed network traffic data* to a threshold, nor is the threshold in that example *known* (i.e., encoded or fixed before monitoring begins).

Defendants' proposed construction should be adopted because it accounts for the entire intrinsic record. *See Network Commerce*, 422 F.3d at 1358-61; *Warner-Lambert Co.*, 418 F.3d at 1340; *Toro Co.*, 199 F.3d at 1300-02; *L.G. Philips*, 2006 U.S. Dist.

---

anonymous FTP, or employees who have departed the company.") [D.I. 268, Ex. O]; Kesidis Tr. 482:6-484:1, 487:3-23 [Godfrey Decl., Ex. D]; *cf.* Porras Tr. 341:25-343:20 [Godfrey Decl., Ex. F]; Valdes Tr. 106:9-17 [Godfrey Decl., Ex. E].

[90] SRI's Br. at 31 (emphasis in original) [D.I. 265].

[91] *See* Kesidis Tr. 482:6-484:1, 487:3-23 [Godfrey Decl., Ex. D].

[92] SRI's Br. at 31 (emphasis in original) [D.I. 265].

[93] *See* '338 patent at 6:60-67 [D.I. 268, Ex. C]; *Statistical Methods* paper at 307 [D.I. 268, Ex. N]; *Live Traffic Analysis* paper at 5-7 [D.I. 268, Ex. O].

LEXIS 38942, at *6-8; *Cephalon, Inc. v. Barr Labs., Inc.*, 389 F. Supp. 2d 602, 604-06 (D. Del. 2005).

Dated: June 30, 2006

POTTER ANDERSON & CORROON LLP

/s/ David E. Moore
Richard L. Horwitz (#2246)
David E. Moore (#3983)
Hercules Plaza, 6th Floor
1313 N. Market Street
Wilmington, DE 19899
Tel.: (302) 984-6000
Fax: (302) 658-1192

OF COUNSEL:
Holmes J. Hawkins III
Natasha H. Moffitt
KING & SPALDING LLP
191 Peachtree St.
Atlanta, GA 30303
Tel: (404) 572-4600
Fax: (404) 572-5100

Theresa A. Moehlman
KING & SPALDING LLP
1185 Avenue of the Americas
New York, New York 10036
Tel.: (212) 556-2100
Fax: (212) 556-2222

Attorneys for Defendant
INTERNET SECURITY SYSTEMS, INC., a Delaware Corporation and INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation

MORRIS, JAMES, HITCHENS & WILLIAMS, LLP

/s/ Richard K. Herrmann
Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
Tel: (302) 888-6800
Fax: (302) 571-1750

OF COUNSEL:
Lloyd R. Day, Jr. (*pro hac vice*)
Robert M. Galvin (*pro hac vice*)
Paul S. Grewal (*pro hac vice*)
DAY CASEBEER MADRID & BATCHELDER LLP
20300 Stevens Creek Blvd., Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

Michael J. Schallop (*pro hac vice*)
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: (408) 517-8000
Fax: (408) 517-8121

Attorneys for Defendant
SYMANTEC CORPORATION

CERTIFICATE OF SERVICE

I hereby certify that on the 12th day of July, 2006, I electronically filed the foregoing document, **REDACTED VERSION OF JOINT CLAIM CONSTRUCTION RESPONSE BRIEF OF DEFENDANTS ISS AND SYMANTEC,** with the Clerk of the Court using CM/ECF which will send notification of such filing to the following:

John F. Horvath, Esq.
Fish & Richardson, P.C.
919 North Market Street, Suite 1100
Wilmington, DE 19801

Richard L. Horwitz, Esq.
David E. Moore, Esq.
Potter Anderson & Corroon LLP
Hercules Plaza
1313 North Market Street, 6th Floor
Wilmington, DE 19801

Additionally, I hereby certify that on the 12th day of July, 2006, the foregoing document was served via email on the following non-registered participants:

Howard G. Pollack, Esq.
Michael J. Curley, Esq.
Fish & Richardson
500 Arguello Street, Suite 500
Redwood City, CA 94063
650.839.5070

Holmes Hawkins, III, Esq.
King & Spalding
191 Peachtree Street
Atlanta, GA 30303
404.572.4600

Theresa Moehlman, Esq.
King & Spalding LLP
1185 Avenue of the Americas
New York, NY 10036-4003
212.556.2100

/s/ Richard K. Herrmann
Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
Morris, James, Hitchens & Williams LLP
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
(302) 888-6800
rherrmann@morrisjames.com

Counsel for Symantec Corporation